

# DeleGate – многофункциональный прокси-сервер

*Сергей Супрунов*

**Современные сети уже почти немыслимы без прокси-серверов. Именно на них возлагаются задачи обеспечения контролируемого доступа в Интернет из локальной сети, экономии трафика за счёт кэширования, а порой и безопасности. Традиционно задача «проксирования» решается отдельно для каждого протокола прикладного уровня специализированными инструментами. Однако иногда оказывается удобнее использовать одно универсальное средство.**

Обычно прокси-серверы работают на прикладном уровне модели OSI. HTTP, FTP, POP3 и прочие протоколы обрабатываются каждый по своим правилам и зачастую своим инструментом. В качестве HTTP-прокси широко используются Squid, OOPS. Они же могут применяться и для работы с FTP-трафиком. Работа по другим протоколам реализуется всевозможными POP3 Proxy, ImapProxy, SMTP Proxy и т. п.

С одной стороны, администратор благодаря такой специализации может выбрать именно те решения, которые ему необходимы. Программа, работающая с одним конкретным протоколом (или несколькими похожими по основным характеристикам), как правило, реализует особенности протокола наиболее полно, что позволяет задействовать практически все его возможности.

Но, с другой стороны, при необходимости обеспечить работу с широким набором различных протоколов, число используемых пакетов может оказаться достаточно большим, усложняя администрирование.

Универсальные же решения, к которым можно отнести так называемые SOCKS-прокси, как правило, ограничиваются модификацией и пере-

сылкой пакетов нижних уровней (TCP/UDP), не вдаваясь в подробности вышележащих протоколов. Как следствие, здесь уже не идёт речь ни о каких дополнительных возможностях, таких как кэширование или фильтрация трафика по признакам, специфичным для тех или иных протоколов (скажем, по HTTP-заголовкам или URL).

Однако есть программа, которая с успехом справляется с проксированием широчайшего набора протоколов, сохраняя при этом большинство их специфических возможностей. Это проект DeleGate, о котором и пойдёт далее речь.

## Знакомство с DeleGate

DeleGate – это универсальный, многоцелевой прокси-сервер, работающий со стеком TCP/IP. Список обслуживаемых им протоколов включает HTTP, FTP, Telnet, NNTP, SMTP, POP, IMAP, LPR, LDAP, ICP, DNS, SSL, Socks, он успешно работает как с IPv4, так и с IPv6. Поддерживает кэширование (для тех протоколов, где это имеет смысл), фильтрацию трафика (интерфейс CFI – Common Filtering Interface), преобразование трафика (скажем, HTTP в HTTPS). Поддерживается PAM-аутентификация и собственный протокол DGAAuth.

Имеются и недостатки (куда же без них). Прежде всего есть некоторые ограничения прозрачного проксирования (из-за жёсткой привязки к HTTP-заголовку «Host:»). Нет поддержки любимого Windows-администраторами протокола аутентификации NTLM (при желании это можно сделать через PAM, но лучше использовать более «прямые» решения). Для каждого соединения создаётся отдельный процесс плюс по дополнительному процессу на каждый фильтр, что отнюдь не прибавляет быстродействия.

DeleGate хотя и распространяется в исходных кодах, не является полностью бесплатным. Однако в небольших сетях он может использоваться без каких-либо отчислений, в том числе и в коммерческих целях (в архиве почтовой рассылки проекта указаны такие ограничения: установка не более чем на 50 хостах, не более 500 внутренних и 50000 внешних пользователей). Для использования в более крупных сетях уже требуется оплата (информации о ценах найти не удалось, видимо, этот вопрос решается индивидуально), однако, на мой взгляд, учитывая то, что каждое соединение обрабатывается в отдельном процессе, использование данного решения в крупных сетях не всегда целесообразно.

## Вопросы установки

С установкой особых проблем возникать не должно. На странице Download можно найти двоичные сборки для Windows, WindowsCE, MacOS X, FreeBSD, Solaris, Zaurus, Linux (правда, обычный ELF-файл, на rpm- или deb-пакеты можете не рассчитывать) и даже для OS/2. При желании можно выполнить сборку вручную.

Рассмотрим процесс установки из исходных кодов версии 9.8.5 (самой свежей на момент подготовки статьи) в системе FreeBSD 6.2 (к слову, DeleGate есть и в коллекции портов, но версия несколько отстаёт от последней; к тому же из-за проблем со скачиванием архива просто так сборка не пройдёт – сперва придётся где-то доставать архив вручную):

```
$ fetch http://delegate.org/anonftp/DeleGate/
$ cd delegate9.8.5
$ tar xzvf delegate9.8.5.tar.gz
$ cd delegate9.8.5
$ make
```

В начале сборки у вас будет запрошен адрес электронной почты администратора, который будет в дальнейшем фигурировать в сообщениях об ошибках.

Цель install в файле Makefile дистрибутива не предусмотрена, поэтому завершить установку вам придётся самостоятельно, для чего нужно будет перенести появившийся двоичный файл src/delegated в каталог постоянного размещения (для FreeBSD наиболее подходящим выглядит /usr/local/sbin).

Полученный демон готов к работе, однако некоторые функции реализованы сторонними библиотеками, сборку которых при необходимости нужно будет выполнить отдельно (см. файл INSTALL дистрибутива).

## Коротко о синтаксисе команды

DeleGate предполагает обычный запуск из командной строки, все параметры работы задаются здесь же:

```
$ delegated -P<порт> -F<функция> <опции> +=<конфиг>
<параметры>
```

Здесь <порт> – номер порта (или номера портов через запятую), который будет обслуживаться данным экземпляром прокси-сервера. С помощью -F можно дать delegated распоряжение выполнить ту или иную функцию (например, остановить другой экземпляр delegated, вывести на экран версию, «прикинуться» telnet-клиентом, выполнить разрешение имени хоста и т. п.; полный список поддерживаемых функций можно просмотреть командой «delegated -Fhelp»).

Среди опций наиболее полезными могут оказаться следующие:

- -f – вынуждает delegated не переходить в фоновый режим и выводить все отладочные сообщения на экран;
- -v – задает уровень отладочных сообщений (может уточняться следующим символом, см. документацию);
- -r – приводит к перезапуску сервера, уже работающего с данными параметрами.



**STAFFCOP**  
www.StaffCop.ru

**ХОТИТЕ ЗНАТЬ,  
НА ЧТО ВАШИ СОТРУДНИКИ  
ТРАТЯТ РАБОЧЕЕ ВРЕМЯ?**

Реклама

**ЕСТЬ СПОСОБ!**

Установите программу

# STAFFCOP

для слежения за компьютером и контроля рабочего времени персонала!

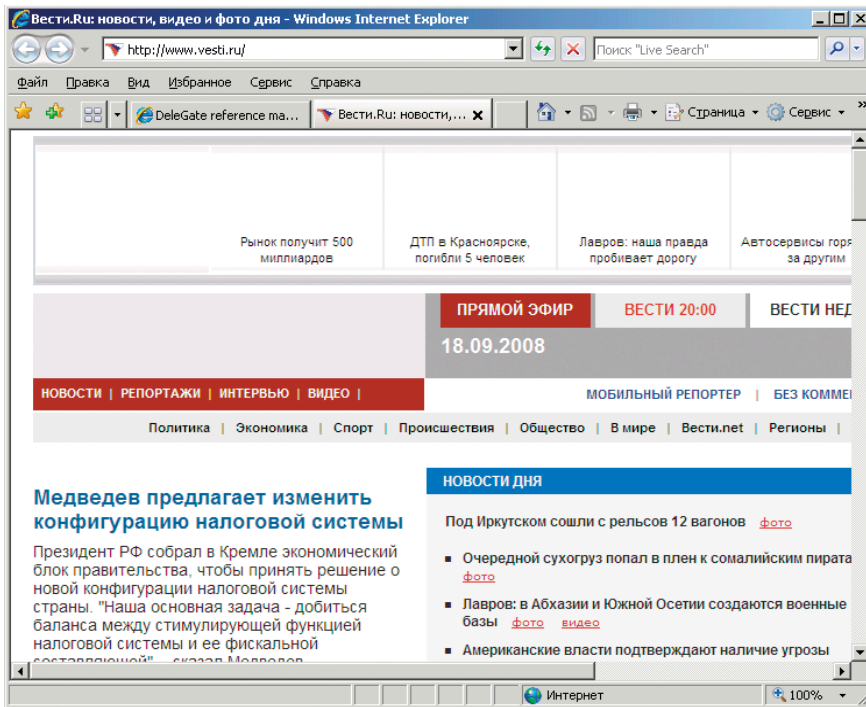


**И ВЫ УЗНАЕТЕ:**

- какие программы запускают пользователи и когда;
- какие сайты они посещают и сколько времени проводят на них;
- с кем и о чём общаются через ICQ, MSN;
- что видят пользователи на экранах своих мониторов;
- какие USB устройства подключают.

**ПОДРОБНОСТИ**  
у наших специалистов:  
+7 (499) 940-47-11, sales@staffcop.ru и на сайте www.StaffCop.ru

\*программа подходит для установки на домашний компьютер

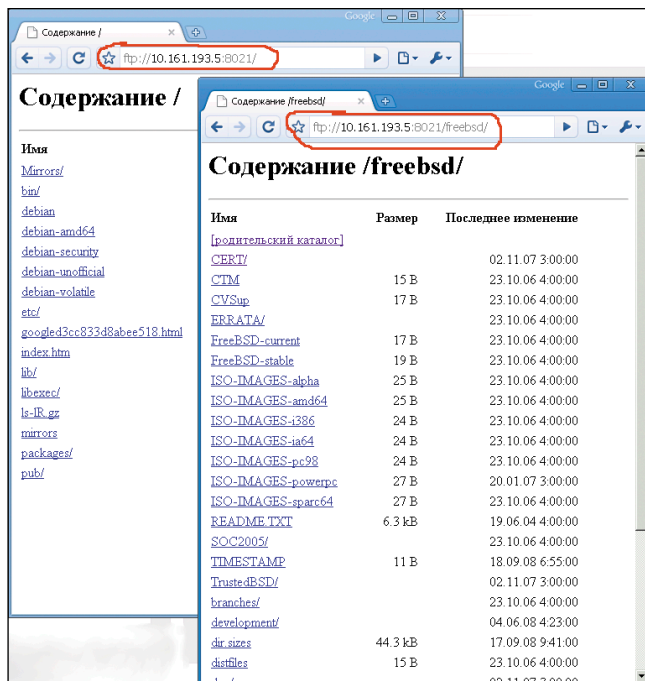


К Примеру 4. Чем меньше картинок, тем больше экономия...

Если параметров слишком много или просто удобно их где-то «зафиксировать», есть возможность создать конфигурационный файл (или несколько) и передать его имя демону при запуске как <конфиг>.

В конфигурационный файл заносятся все необходимые параметры, по одному в каждой строке. Не забывайте сохранять дефис перед теми параметрами, которым он требуется.

Наконец, <параметры>, – это основная часть, влияющая на характер работы прокси-сервера: по какому протоколу он будет работать, включать ли кэширование и т. п. Зада-



К Примеру 6. Хотя каталога freebsd в листинге не видно, но по прямому URL он доступен

ются в виде пар «ИМЯ=значение», например, параметр «SERVER=http» означает, что DeleGate будет выполнять роль HTTP-прокси:

```
$ delegated -P8080 SERVER=http
```

Данная команда запустит простой HTTP-прокси на порту 8080. Остановить запущенный прокси-сервер можно следующей командой, передав в качестве аргумента тот же порт, который использовался в команде запуска:

```
$ delegated -P8080 -Fkill
```

Кстати говоря, delegated можно запускать от имени непривилегированного пользователя за исключением случая, когда права root являются необходимыми (например, для привязки к порту с номером ниже 1024). Ознакомиться со всеми возможностями DeleGate вы сможете в объемном,

65-страничном руководстве. Мы же ограничимся рассмотрением нескольких типовых (и не очень) решений.

## Примеры решений

Для дальнейших примерах будем считать, что myserver.ru – это имя вашего сервера (на котором запущен DeleGate).

### Пример 1. Обычный кэширующий HTTP-прокси

Для начала запустим самый обычный прокси-сервер с кэшированием:

```
$ delegated -P192.168.0.254:8080 SERVER=http CACHE=do
```

Принимать соединения от клиентов сервер будет на внутреннем интерфейсе 192.168.0.254, на порту 8080. Работа будет вестись по протоколу HTTP, кэширование будет осуществляться (по умолчанию кэш располагается в <userhomedir>/delegate/cache или в /var/spool/delegate/cache, изменить это можно параметром CACHEDIR).

Кстати, небольшой фокус: можно не настраивать браузер на использование прокси, а работать через него, используя URL вида «http://192.168.0.254:8080/\_http://nettools.ru/», где 192.168.0.254 – хост, на котором запущен DeleGate (на 8080-м порту), а nettools.ru – запрашиваемый ресурс. Все ссылки автоматически будут преобразованы к такому же виду, так что на удобстве дальнейшей работы с сайтом этот приём никак не отразится. Это может быть удобно в тех случаях, когда прокси-сервер требуется лишь временами.

### Пример 2. DeleGate как веб-сервер

Вы можете использовать DeleGate и в качестве «оригинального» веб-сервера:

```
# delegated -P80 SERVER=http MOUNT="/* /var/www/*" _
RELAY=no RELIABLE=""
```



Теперь DeleGate будет ждать HTTP-запросы на 80-м порту, сопоставляя все запрошенные файлы (\*) файлам в каталоге /var/www. Параметром RELAY=no мы запрещаем демону выполнять роль прокси-сервера, RELIABLE указывает список адресов, с которых запросы можно принимать (в нашем случае – отовсюду).

Файлы с расширением .cgi будут обрабатываться по протоколу CGI (конечно, при условии, что cgi-файл будет исполняемым; в противном случае клиенту будет возвращена страница ошибки – the service is unavailable temporarily), все остальные файлы – выдаваться клиенту как есть.

При желании можно явно указать отдельный cgi-каталог (это задаётся в параметре монтирования):

```
MOUNT="/cgi/* cgi:/var/www/cgi-bin/*"
```

Есть ещё множество различных опций (см. в документации описание параметров HTTPCONF, CGIENV и т. п.

Хотя DeleGate и не заменит вам полноценный веб-сервер, но, как видите, для решения несложных задач выдачи преимущественно статического веб-контента вполне можно обойтись и без Apache.

### Пример 3. «Маскировка» удалённого сервера

DeleGate позволяет выдавать себя за некоторый удалённый сервер (т.е. выполнять роль reverse-proxy). Например, выполняем следующую команду:

```
# delegated -P80 SERVER=http://www.samag.ru PERMIT="*"
```

В результате при обращении на 80-й порт нашего сервера (запросом http://myserver.ru) пользователю будет выдана стартовая страница сайта www.samag.ru.

Аналогично по запросу http://myserver.ru/forum/index.php/topic,825.0.html откроется http://www.samag.ru/forum/index.php/topic,825.0.html.

В адресной строке браузера клиента будет везде фигурировать именно myserver.ru, и у пользователя должно сложиться впечатление, что myserver.ru – это и есть сайт «Системного администратора».

Пример 4. Фильтрация html-тегов

### Пример 4. Фильтрация html-тегов

Пытайтесь приучить своих пользователей ходить в Интернет только с помощью Opera с отключенными изображениями, но они никак не проникаются необходимостью экономить трафик? Есть жёсткое и надёжное решение:

```
$ delegated -P8080 SERVER=http HTTPCONF=kill-tag:IMG
```

Теперь в любом браузере от изображений не останется и следа (если точнее, то в исходном коде теги <img ...> будут заменены на <killed-img ...> и соответственно отображаться не будут). Возможности параметра HTTPCONF этим не ограничиваются – он умеет модифицировать заголовки, задавать тайм-ауты, ограничивать методы запросов (например, можно разрешить только GET-запросы) и т. д. Читайте Reference Manual.

### Пример 5. Прокси-сервер FTP

Простейший запуск FTP-прокси выполняется следующей командой:

```
$ delegated -P8021 SERVER=ftp
```

Прокси-сервер будет успешно работать как в активном, так и в пассивном режимах. Причём работа будет возможна даже в том случае, если используемый FTP-клиент не поддерживает работу через прокси: в качестве FTP-сервера ему нужно будет передать адрес и порт, на которых работает DeleGate, а имя пользователя указать в виде user@remote.host. При необходимости можно включить кэширование (параметром CACHE=do).

### Пример 6. Монтирование нескольких FTP-серверов в один

Рассмотрим следующую команду:



## Российский стандарт архивации! Проверенное качество сжатия и безопасность

Реклама

**База знаний:** <http://win-rar.ru/support/knowledge/>  
**FAQ:** <http://win-rar.ru/support/faq/>

Получить подробную информацию о программном продукте WinRAR можно на сайте: <http://www.softkey.ru>

#### Возможности WinRAR:

- управление RAR и ZIP архивами, работа с другими форматами (CAB, ARJ, LZH, TAR, GZ, ACE, UUE, BZ2, JAR, ISO, 7Z, Z);
- поддержка непрерывных архивов с увеличенной степенью сжатия;
- поддержка многотомных архивов;
- продвинутый самораспаковывающийся модуль;
- 128-битная криптографическая защита и электронные подписи архивов;
- возможность восстановления/резервного копирования исходных данных;
- поддерживаются Windows, DOS, OS/2, Linux, FreeBSD, MACOSX и платформы карманных ПК;
- одна лицензия позволяет использовать продукт на любых платформах и в разных языковых версиях;
- БЕСПЛАТНОЕ получение ВСЕХ новых версии WinRAR в течение неограниченного времени.

SoftKey —  
эксклюзивный дистрибутор  
WinRAR в России



```
# delegated -P21 SERVER=ftp://ftp.chg.ru MOUNT="/freebsd/*"
ftp://ftp.freebsd.org/pub/FreeBSD/*"
```

Здесь мы на 21-м порту запускаем «маскирующий» FTP-прокси, который будет выдавать себя за ftp.chg.ru. Дополнительно монтируется каталог pub сервера ftp.freebsd.org таким образом, что он будет доступен при запросе ресурса ftp://myserver.ru/freebsd. (Правда, должен заметить, что при подключении по адресу ftp://myserver.ru данной папки в листинге каталога видно не будет – там будут представлены лишь каталоги «основного» сервера ftp.chg.ru).

### Пример 7. Трансляция FTP в HTTP

Раз DeleGate умеет работать и с FTP, и с HTTP, то почему бы эти способности не совместить?

```
$ delegated -P192.168.0.254:8080 SERVER=http
MOUNT="/* ftp://ftp.chg.ru/*"
```

В результате клиент сможет работать по протоколу HTTP с указанным FTP-сервером.

### Пример 8. DeleGate как DNS-сервер

Помимо работы в качестве «оригинального» HTTP- и FTP-серверов, DeleGate способен функционировать и как DNS-сервер. В качестве источника информации о «зонах» он может использовать реальный DNS-сервер либо файл в формате /etc/hosts. Второй случай будет выглядеть так:

```
# delegated -P53 SERVER=dns RESOLV=file:/etc/hosts
```

Очень удобно, если из локальной сети хочется работать с некоторыми хостами по имени, но настраивать из-за этого DNS-сервер лень. Помимо файла /etc/hosts, можно использовать карты NIS, указав «RESOLV=nis».

### Пример 9. Использование основного и резервного SMTP-серверов

Предположим, что вы можете использовать для отправки почты один из двух SMTP-серверов, но основной работает не всегда, а постоянно использовать резервный нежелательно... DeleGate поможет и в этом случае:

```
# delegated -P25 SERVER=smtp
CLUSTER=smtp://mail.first.ru,mail.second.ru
```

Благодаря объявлению кластера DeleGate, получив запрос на 25-й порт, будет последовательно пробовать перечисленные в данном параметре серверы, пока не найдёт работоспособный. Например, если с mail.first.ru что-то случится, запросы будут пересылаться на mail.second.ru. В настройках клиента нужно будет указать в качестве сервера исходящих сообщений хост, на котором запущен DeleGate.

### Пример 10. Трансляция Telnet в SSH

Хотите работать с удалёнными SSH-серверами, используя какой-нибудь Telnet-клиент? Не знаю, зачем такое может понадобиться (экономить таким образом вычислительные ресурсы настольного компьютера сейчас смешно, а ходить с сотового телефона по Telnet даже до прокси-сервера слишком небезопасно), но тем не менее DeleGate это позволяет:

```
$ delegated -P8023 SERVER=telnet://admin@-ssh.192.168.3.220
```

Теперь по команде «telnet myserver 8023» вам предложат ввести пароль пользователя admin на машине 192.168.3.220, с которой работа будет вестись уже по протоколу SSH (на участке между DeleGate и данным хостом). Обратите внимание, что соединение между клиентом и DeleGate останется незащищённым! На мой взгляд, более полезной была бы трансляция «SSH → Telnet» (что позволило бы из дома безопасно работать с оборудованием, понимающим только Telnet), но такой возможности у DeleGate мне обнаружить не удалось.

### Пример 11. Простейший SOCKS-сервер

Решается задача просто, как и в предыдущих случаях:

```
$ delegated -P192.168.0.254:8111 SERVER=socks
```

Теперь на 8111-м порту у вас будет работать SOCKS-сервер, причём он сможет обрабатывать запросы как socks4, так и socks5. Если необходимо конкретизировать используемый протокол, в параметре SERVER можно явно указать тип сервера – socks4 или socks5.

### Пример 12. Прокси-сервер посложнее

На «закуску» рассмотрим пример более функционального прокси-сервера. Пусть в его задачи входит следующее:

- обеспечить работу по протоколам HTTP, HTTPS и FTP на одном порту;
- требовать от пользователей аутентификацию (будем использовать возможности PAM);
- осуществлять кэширование;
- вести лог-файл;
- блокировать доступ к ресурсам в определённой доменной зоне;
- ограничить разрешённый контент лишь несколькими MIME-типами.

В данном случае удобнее использовать конфигурационный файл:

```
$ cat httpproxy.conf
-P8080
SERVER=http
CACHE=do
RELIABLE=192.168.0.0/24
AUTHORIZER=-pam/passwd
PROTOLOG="/usr/home/serg/delegate/var/httpproxy.log:%C"
OWNER=serg
FTOCL="/usr/home/serg/delegate/etc/onlymime.cfi"
REJECT="http:*.*mobi:*"

$ delegated +=httpproxy.conf
```

DeleGate достаточно разумен, чтобы по типу запроса разобраться, к какому протоколу он относится, так что одного порта вполне достаточно.

Небольшое замечание по авторизации: поскольку мы используем PAM (авторизация будет выполняться по системной базе учётных записей), delegated должен иметь необходимые привилегии. Этого можно достичь либо запуском от имени root (дополнительно нужно будет указать параметр «OWNER=root», чтобы delegated не переключал

ся на непривилегированного пользователя), либо собрав и установив дополнение dgauth:

```
# cd delegate9.8.5/subin
# make install
```

В результате в каталоге \$DGROOT/subin появятся несколько файлов. Нужно проверить, что \$DGROOT совпадает с тем, который использует delegated. Это видно при запуске:

```
$ delegated +=httpproxy.conf
```

```
<DeleGate/9.8.5> [90863] -P8080 READY
Config: FreeBSD/6.2-RELEASE-p4; FileSize-Bits=64/64,64/32,32;
socket=65536/32768; sockpair=8192/8192,1016++U; thread=PThread/
pthread; stty=tcsetattr; umem=127/187/0M
DGROOT=/home/serg/delegate
ADMIN=support@myserver.ru
```

Изменить \$DGROOT можно, добавив в конфигурационный файл соответствующий параметр: «DGROOT=/var/delegate».

Теперь небольшое отступление о лог-файле. Как нетрудно догадаться, настраивается его ведение параметром PROTOLOG. В данном случае мы указываем имя лог-файла и его формат (%C соответствует «стандартному» формату CERN-HTTPD; о других возможных форматах можно узнать из документации). При запуске с ключом -f все сообщения будут выводиться на экран вместо записи в файл. Очевидно, что процесс delegated должен иметь достаточно прав для создания указанного в параметре PROTOLOG файла. В частности, для этого я использую параметр «OWNER=serg», чтобы delegated не «опускался» при старте до уровня nobody.

Для решения задачи ограничения допустимого контента удобно использовать CFI-фильтр, чем мы и воспользовались (параметр FTOCL можно расшифровать как «Filter TO CClient», т.е. фильтровать то, что идёт к клиенту; аналогично есть параметры FFROMCL, FTOSV и FFROMSV, а также независимые от направления FCL и FSV). Сам фильтр выглядит следующим образом:

```
$ cat /usr/home/serg/delegate/etc/onlymime.cfi
```

```
#!cfi
Content-Type: text/plain
Content-Type: text/html
Content-Type: image/gif
Content-Type: image/png
Content-Type: image/jpeg
```

То есть мы перечисляем допустимые MIME-типы. Ответ, не содержащий в заголовке один из указанных типов, будет отклонён. Аналогично можно выполнять фильтрацию по некоторым другим полям заголовка (пока этот список ограничен, см. документацию), по телу сообщения. Поддерживаются некоторые «действия» (скажем, модифицировать ту или иную часть сообщения). Можно подключать внешние фильтрующие программы (которые принимают некоторый текст на входе и возвращают модифицированный; для простейших преобразований вполне можно использовать

## «За кадром»

В данной статье остались без детального рассмотрения такие вопросы, как аутентификация с помощью DeleGate, каскадное подключение нескольких прокси-серверов, взаимодействие с другими прокси (DeleGate можно использовать для маршрутизации, когда разные запросы отправ-

ляются к разным вышестоящим прокси-серверам), фильтры, туннели, компрессия, трансляция TCP↔UDP, IPv4↔IPv6. Всё это DeleGate умеет, информацию можно найти в документации, идущей в составе дистрибутива, а также доступной на сайте проекта.

Имеются и другие возможности, в которые мы, пожалуй, вдаваться не будем. Для блокирования доступа к ресурсам зоны mobi (нет, она ничем не провинилась... просто нужно же на чём-то пример показать?) был использован параметр REJECT. Формат его следующий:

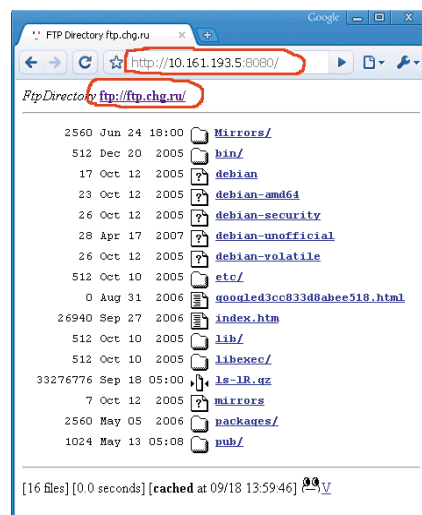
```
REJECT=<список протоколов>:<запрашиваемые хосты>: ␣
<хосты-клиенты>
```

Как видите, параметр достаточно гибок, чтобы блокировать доступ по тому или иному протоколу к различным ресурсам разным клиентам. От «запретить лично Васе заходить на этот конкретный сайт по FTP» до «запретить всем всё».

## Итоги

Как видите, DeleGate действительно способен на многое. Не скажу, что он впечатляюще быстр или абсолютно не требователен к ресурсам. Не скажу, что он на все 100% заменит вам Squid и POP3Proxy. Не скажу, что, используя его, вы никогда не столкнётесь с ошибками. Но то, что это удобное, «мобильное», функциональное средство для быстрого решения большинства типовых задач, факт, думаю, неоспоримый. ●

1. Официальный сайт проекта – <http://www.delegate.org>.
2. Пример использования DeleGate в качестве POP3-прокси с фильтрацией спама – <http://www.deepsea.force9.co.uk/pop3proxy.html>.
3. Пример запуска CMS Skeletonz через DeleGate – [http://orangoo.com/skeletonz/User\\_guide/Running\\_Skeletonz\\_behind\\_Delegate](http://orangoo.com/skeletonz/User_guide/Running_Skeletonz_behind_Delegate).



К Примеру 7. Работа с FTP-сервером по протоколу HTTP